2, rue du Plessis
35 770 VERN SUR SEICHE

Téléphone : 02 .99 .04 .89 . 00 Télécopie : 02 .99 .04 .89 . 01

SOFREL S4W - CSPN

Cible de sécurité

Référence ..... : **S4-CSPN-CibleDeSécurité.docx**

Version ..... : **V1.32 publique**

Date ..... : **vendredi 11 juin 2021**

Portée ..... : **Publique**

Auteur(s) ..... : **T. FLOC'H ; J.M. ADOUE**

Validation ..... : **J.M. MERIC ; J.L. BOBET**

SOMMAIRE

REFERENCES DOCUMENTAIRES

[MET-CC] Méthodologie d'évaluation des fonctions de sécurité de produit selon les Critères Communs : https://www.ssi.gouv.fr/entreprise/produits-certifies/cc/criteres-et-methodologies-devaluation/

[MET-CSPN] Méthodologie d'évaluation des fonctions de sécurité de produit selon la CSPN, Agence nationale de la sécurité des SI (ANSSI) : https://www.ssi.gouv.fr/entreprise/produits-certifies/produits-certifies-cspn/les-procedures-formulaires-et-methodologies/

[PP-PLC-MT-1.1] Profils court et moyen terme de protection pour les systèmes industriels : https://www.ssi.gouv.fr/guide/profils-de-protection-pour-les-systemes-industriels/ :

- Automate court terme v1.1-fr.pdf
- Automate moyen terme v1.1-fr.pdf

1. INTRODUCTION

1.1 Objet du document

Ce document établit la cible de sécurité dans le cadre de la certification CSPN[1] du produit « **Poste local de télégestion S4W** (RTU[2]) » conçu par la société **LACROIX-Sofrel**.

Cette cible de sécurité est inspirée du profil de protection « moyen terme » d'un produit de type Automate Programmable Industriel (API ou PLC[3]), [PP-PLC-MT-1.1], défini par l'ANSSI. Toutefois, compte tenu des différences importantes entre le poste local de télégestion (RTU) et un PLC, nous avons rédigé cette cible de sécurité pour tenir compte des spécificités des installations que nous pilotons.

En effet, notre produit se différencie largement d'un PLC dans son mode d'utilisation et d'installation :

- Un PLC est installé dans une usine, et sa portée de communication se limite à un réseau IP local.
- Un poste local de télégestion :
  - Fonctionne sur un réseau distribué : il s'installe sur des sites géographiquement isolés (château d'eau, réservoir, station de pompage, poste de relèvement, …) ;
  - Communique à distance avec des postes centraux de télégestion (SCADA[4],…) ou des utilisateurs ;
  - Utilise différents supports de communication :
    - Majoritairement des réseaux cellulaires GSM (IP / SMS)
    - Mais aussi des réseaux ADSL via une connexion Ethernet
  - Fonctionne aussi bien sur un réseau privé que sur le réseau public (Internet).

Figure 1 : Télégestion d'un réseau d'eau

[1] Certification de Sécurité de Premier Niveau
[2] RTU (Remote Terminal Unit)
[3] PLC (Programmable logic Controller)
[4] SCADA : Poste central de télégestion

1.2 Identification du produit

Fabricant	LACROIX-Sofrel 2, rue du Plessis 35770 VERN SUR SEICHE - FRANCE
Lien entreprise	https://www.lacroix-sofrel.fr
Lien produit	https://www.lacroix-sofrel.fr/offre/postes-locaux/s4w/
Produit	Poste local de télégestion S4W
Version logicielle	V3.10.41.100
Version matérielle	SF 002 310x[5]
Paramètres fixes	Produit 1 : - Numéro de série produit : SF0023103000266 - Adresse MAC : 00:0B:48:70:01:68 - Numéro IMEI : 359515054615822 Produit 2 : - Numéro de série produit : SF0023103000282 - Adresse MAC : 00:0B:48:70:01:E3 - Numéro IMEI : 359515054446103

2. DESCRIPTION DU PRODUIT

2.1 Description générale

Le *« **Poste Local de Télégestion S4W** »* (ci-dessous référencé S4W) est un équipement permettant de surveiller 24h/24h et contrôler à distance, l'ensemble des installations techniques réparties sur les réseaux d'eau potable et d'assainissement.

Ces réseaux comprennent de nombreux ouvrages souvent isolés géographiquement (captages, réservoirs, stations de pompage, usine de traitement, …). Compte tenu du nombre d'ouvrages à surveiller, il est impossible d'y maintenir du personnel à demeure. Pour faire face à ces contraintes, des S4W sont donc installés sur les différents sites et permettent ainsi de superviser ces ouvrages à distance depuis un réseau de supervision.

Les S4W acquièrent, traitent et transmettent les données des différents organes de captage de ces ouvrages (états de marche et d'arrêt, défauts, mesures de niveau et de pression, taux de chlore, comptages, température, …). Ils enregistrent en permanence les événements qui se produisent sur l'installation. Ainsi, le personnel qui exploite le réseau dispose de toutes les données nécessaires à une gestion optimale de ses installations.

Un réseau de télégestion est doté d'un « *Poste Central de Télégestion* » (ou SCADA) qui a pour rôle de centraliser les données acquises par les S4W sur les différentes installations. Le Poste Central de Télégestion permet au personnel d'exploitation d'obtenir une vue globale du fonctionnement de ses installations et ainsi de maîtriser et d'optimiser son fonctionnement.

[5] Numéro de version matérielle utilisé comme préfixe du numéro de série produit.
3101 : S4W 8 DI, 2 AI, 2 DO
3103 : S4W 16 DI, 4 AI, 4 DO

A la différence d'un Automate Programmable Industriel (API), le S4W est préprogrammé et ne nécessite donc pas de programme fourni par l'utilisateur pour assurer les services d'acquisition, de traitement, d'archivage des entrées/sorties et de communication. Il suffit de configurer les services. Il peut, néanmoins, accepter un programme d'automatisme écrit par l'utilisateur pour compléter les services déjà existants.

En outre, la fonction « report d'alarmes » de S4W assure l'envoi d'alarmes vers le Poste Central de Télégestion et le personnel d'astreinte, sous forme de SMS[6] et/ou d'Email[6].

[6] Hors cible

La ToE[7] considérée est le S4W développé par LACROIX-Sofrel

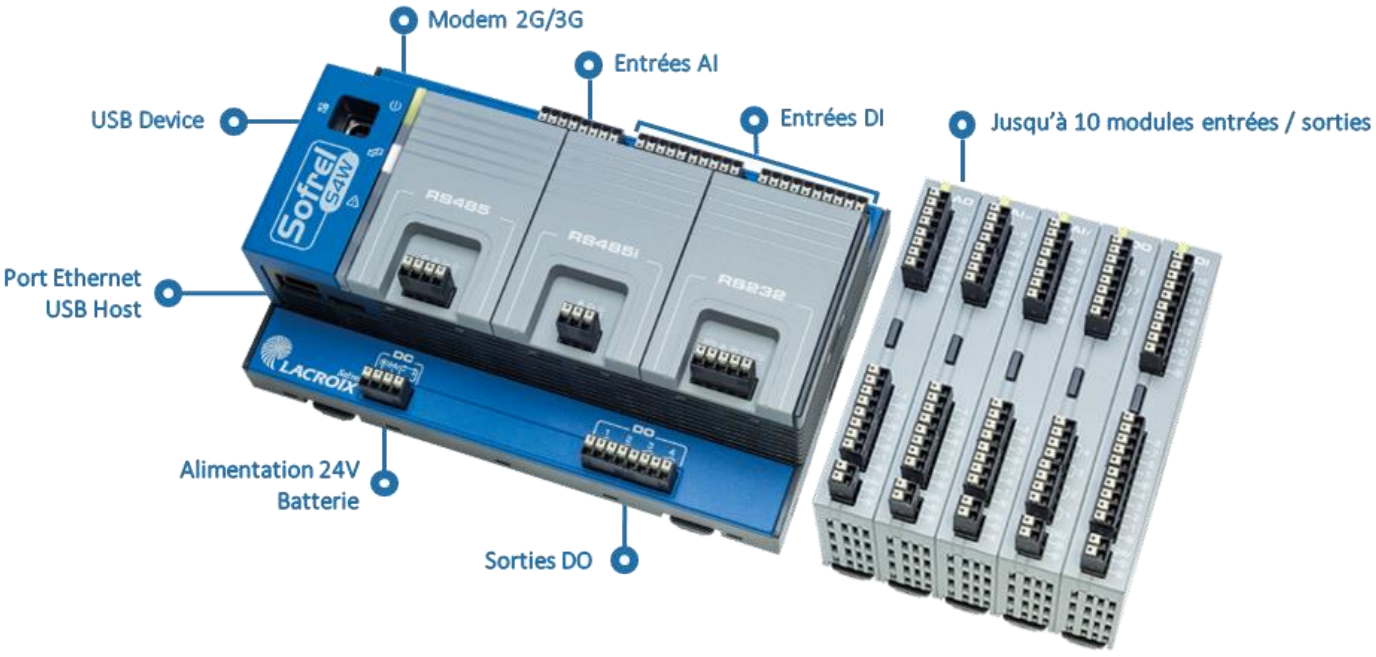

Figure 2 - S4W

Le S4W interagit avec :

1. Des équipements déployés sur son propre réseau de terrain

Equipement	**Interface physique**						
	Entrées / sorties	**RS232**	**RS485**	**USB Device**	**USB Host**	**Ethernet**	**GSM**
Capteurs et actionneurs *Acquisition et restitution de données*	X						
Régulateurs *Acquisition et restitution de données*		X	X				
Débitmètres *Acquisition de données*		X	X				
PLC *Acquisition et restitution de données*		X	X			X[8]	
Compteurs *Acquisition de données*		X	X				

[7] Target of Evaluation
[8] Uniquement si le port Ethernet est exclusivement connecté au réseau de terrain (sans interconnexion avec le réseau de supervision).

2. Des équipements déployés sur un réseau de terrain distant

Equipement	Interface physique						
	Entrées / sorties	RS232	RS485	USB Device	USB Host	Ethernet	GSM
Autres S4W *Acquisition et restitution de données*						X	X

3. Des équipements d'exploitation, d'administration, et de supervision, locaux ou distants :

Equipement	Interface physique						
	Entrées / sorties	RS232	RS485	USB Device	USB Host	Ethernet	GSM
S4-Display *Exploitation, visualisation*					X		
S4-View *Exploitation, visualisation, diagnostic*				X		X	X
S4W-Tools *Configuration*				X		X	X
S4-Manager *Mise à jour de la liste des utilisateurs (personnes physiques) et de leurs droits d'accès*						X	X
Poste central de télégestion *Supervision des installations*						X	X
Serveur Syslog *Surveillance des installations*						X	X

2.2 Description des fonctions du produit

La ToE intègre les fonctions suivantes :

1. **Exécution du programme** : de base la ToE exécute un programme préchargé dans le logiciel. Elle peut aussi exécuter un programme d'automatisme fourni par l'utilisateur pour compléter les services déjà existants.
2. **Gestion des entrées/sorties** : la ToE est capable de communiquer pour lire ou écrire sur des entrées/sorties locales ou déportées et connectées sur un autre S4W. Ces entrées/sorties peuvent être logiques ou analogiques. Elles permettent à la ToE de contrôler et de commander le processus industriel.
3. **Communication avec la supervision :** la ToE peut communiquer avec le Poste Central de Télégestion pour recevoir des ordres et remonter des informations sur le processus industriel.
4. **Administration de la ToE** : la ToE dispose de services d'administrations permettant de configurer ou, dans certains cas, de programmer l'ensemble des autres fonctionnalités.

   Les interfaces d'administration sont disponibles au travers des outils **S4W-Tools** et **S4-Manager**.
5. **Exploitation de la ToE** : la ToE dispose de services permettant l'exploitation de ses données, et la réalisation d'opérations de diagnostic.

   Les interfaces d'exploitation sont disponibles au travers des outils **S4-View** et **S4-Display.**
6. **Journalisation locale d'évènements** : la ToE permet de définir une politique de journalisation locale d'évènements notamment de sécurité et d'administration. Ces évènements sont consignés dans un journal local appelé « **Journal de fonctionnement »**.
7. **Journalisation distante d'évènements** : la ToE permet de définir une politique de journalisation distante d'évènements notamment de sécurité et d'administration. Ces évènements sont consignés sur un serveur Syslog distant.
8. **Gestion d'alarmes** : la ToE permet, au travers de sa configuration, d'identifier des données qui, en fonction de leur état, génèrent des alarmes vers le Poste Central de Télégestion et/ou un autre destinataire (SMS, …). Ces alarmes doivent être acquittées par les destinataires pour signifier leur bonne prise en compte.

2.3 Descriptif de l'utilisation du produit

La ToE gère ses propres entrées-sorties en interne (produit compact). Il est possible d'étendre les capacités de la ToE en ajoutant jusqu'à 10 modules d'entrées/sorties sur un bus dédié. Il est également possible de connecter une interface homme-machine (S4-Display) sur le port USB Host de la ToE, pour effectuer des opérations d'exploitation (lecture/écriture de données, visualisation d'archives, acquittement d'alarme).

Des échanges vers le **Poste Central de Télégestion** se font au travers d'interfaces de communication IP de la ToE (GSM/Ethernet). Une perte de liaison entre le **Poste Central de Télégestion** et la ToE n'est pas critique dans le sens où ceci n'a pas d'incidences sur le système industriel sous-jacent (bon fonctionnement des capteurs, actionneurs, etc.). Une perte de connexion d'une journée est acceptable.

L'administration de la ToE se fait avec un ensemble d'outils d'administration :

- **S4W-Tools** pour la gestion de la configuration de la ToE, la mise à jour de la liste des utilisateurs (login, mot de passe et profil) et la mise à jour du logiciel ;
- **S4-Manager** pour la mise à jour de la liste des utilisateurs (login, mot de passe et profil).

Lacroix SOFREL recommande l'utilisation exclusive de S4-Manager pour la mise à jour de la liste des utilisateurs.

L'exploitation de la ToE se fait avec un ensemble d'outils d'exploitation :

- **S4-View** pour la lecture/écriture de données, lecture des archives et des journaux, acquittement des alarmes et services de diagnostic.
- **S4-Display** pour la lecture/écriture de données, lecture des archives et acquittement des alarmes.

La ToE externalise les évènements d'administration et de sécurité vers un serveur Syslog. Dans un cas d'usage standard, la ToE est installée sur un site déporté du réseau de supervision, intégrant le Poste Central de Télégestion, le serveur Syslog, et le S4-Manager, cf.

Figure 3. Les communications s'effectuent en IP, au travers :

- d'un **réseau privé** mis à disposition par un opérateur ;
- du **réseau public (Internet)**.

Pour sécuriser les échanges passant sur le réseau public (GSM et/ou Ethernet), l'utilisateur doit installer sur le réseau de supervision un **serveur VPN compatible OpenVPN**, tel que le serveur **VPN LACROIX Sofrel SG4000**.
Ainsi, pour assurer une communication sécurisée entre la ToE et les machines situées en dehors du réseau local, la ToE :

- établit au préalable un lien VPN avec le serveur VPN
- utilise ensuite ce lien VPN pour communiquer avec les équipements installés sur le réseau de supervision, ou sur un réseau de terrain distant

S4-Display est installé sur la façade avant de l'armoire électrique qui intègre la ToE. Cette installation ne laisse donc apparaître aucune connectique entre la ToE et le S4-Display tant que l'armoire reste fermée.

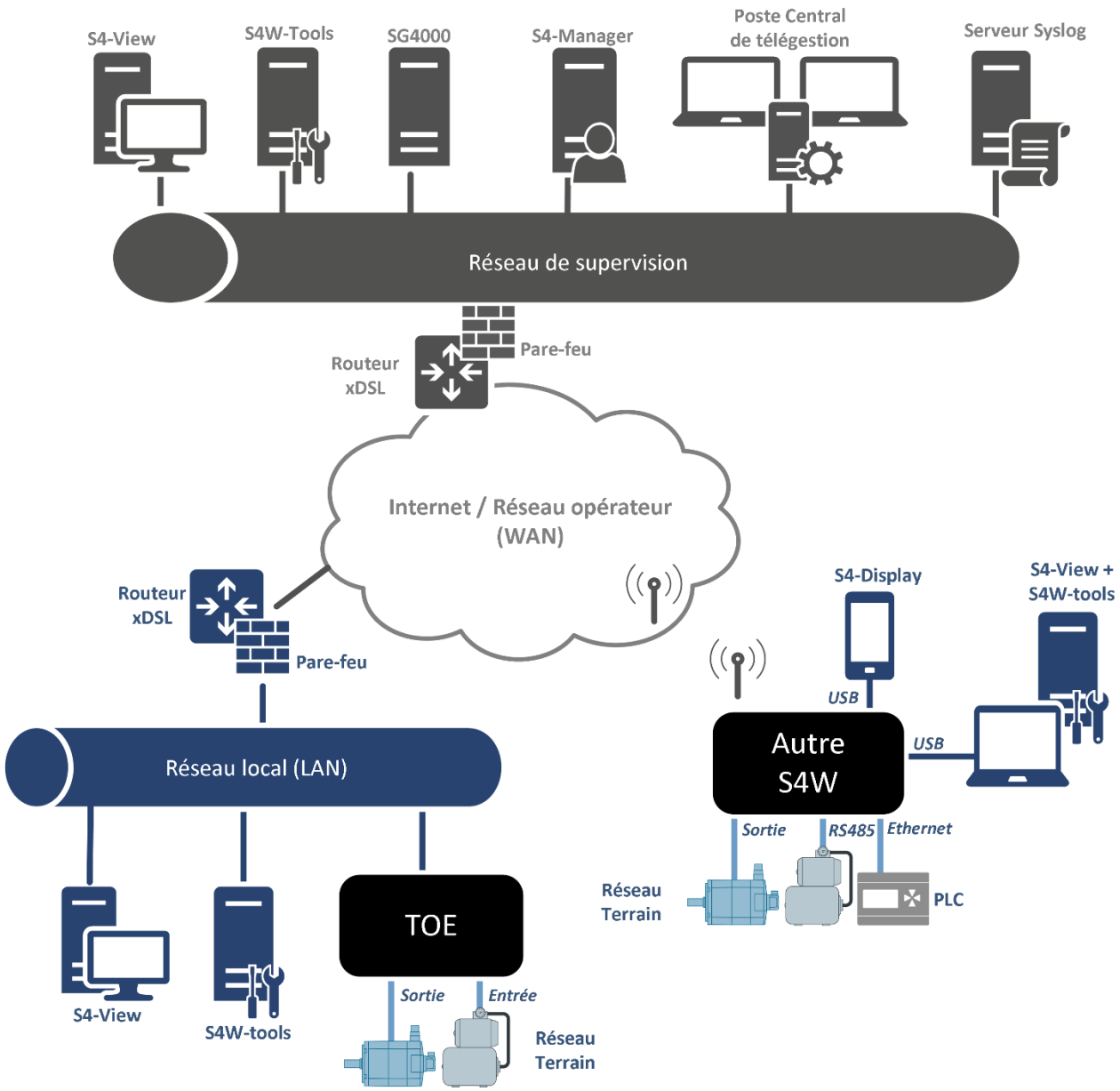

Figure 3 – Architecture physique du réseau pour la ToE, utilisée dans le cadre de l'évaluation

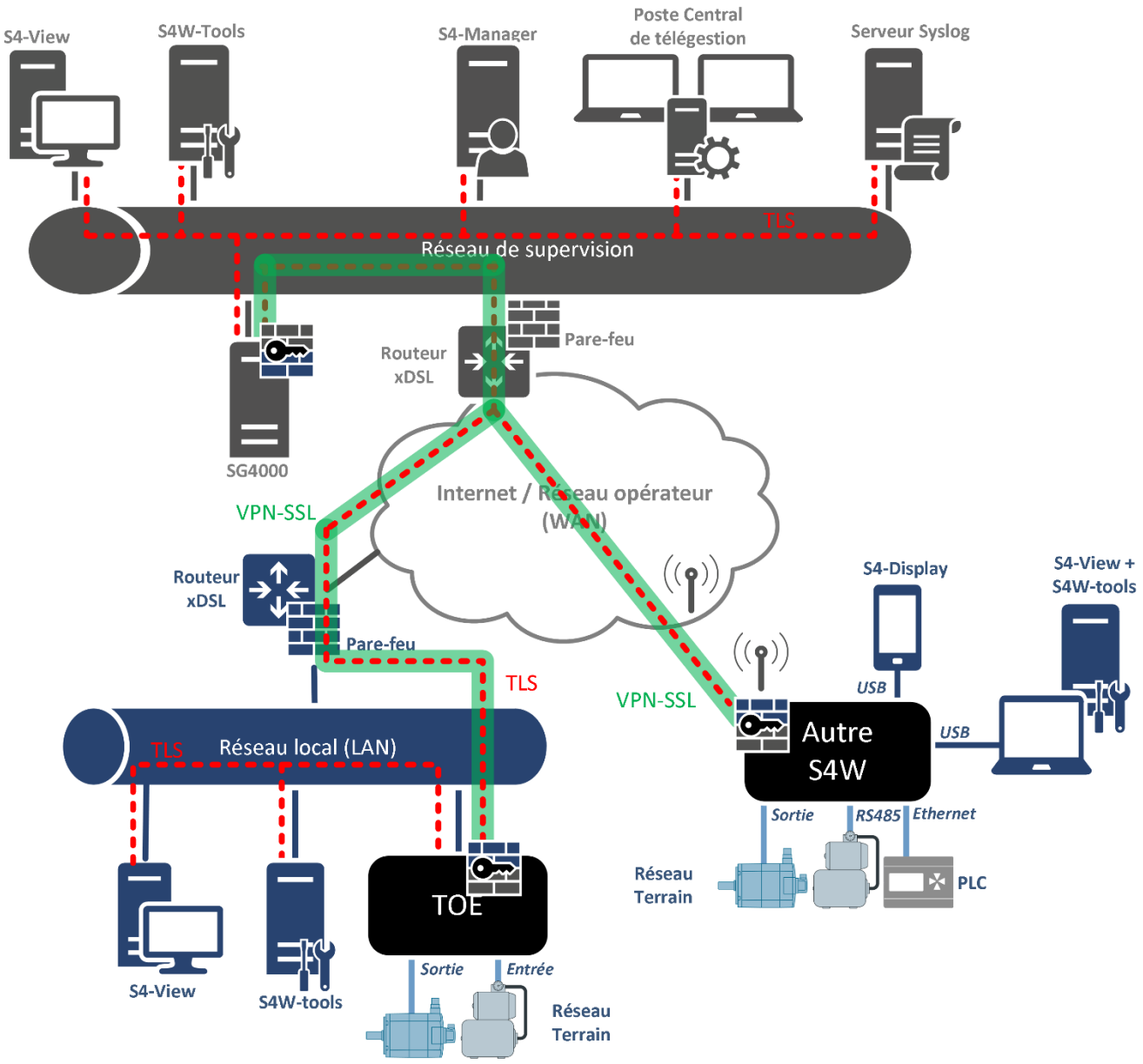

Figure 4 - Architecture logique du réseau pour la ToE, utilisée dans le cadre de l'évaluation

3. PROBLEMATIQUE DE SECURITE

3.1 Descriptif des différents utilisateurs

3.1.1 Personnes physiques

Chaque personne physique est caractérisée par un ou plusieurs comptes, comportant :

- un login unique dans la ToE
- un nom d'utilisateur
- un profil utilisateur
- un mot de passe

Chaque personne physique interagit avec la ToE au travers des outils S4W-Tools, S4-View et S4-Display. Son profil utilisateur détermine des droits d'accès sur les éléments suivants :

- Lecture et écriture des données métier
- Lecture du journal local
- Ecriture de la configuration
- Acquittement des alarmes
- Mise à jour du logiciel
- Services de diagnostic (demande de redémarrage, lecture des informations réseau, état des cartes de communication, forçage des entrées/sorties …)
- Mise à jour de la liste des utilisateurs

Les profils utilisateur des personnes physiques susceptibles d'interagir avec la ToE sont les suivants :

Fonction accessible	Profil utilisateur				Outil[9]		
	Consultant	Exploitant	Administrateur	Manager	S4W-Tools	S4-View	S4-Display
Lecture des données métier	X	X	X	X		X	X
Ecriture des données métier		X	X	X		X	X
Lecture du journal local	X	X	X	X		X	
Effacement du journal local			X	X		X	
Acquittement des alarmes		X	X	X		X	X
Ecriture de la configuration			X	X	X		
Mise à jour du logiciel			X	X	X		
Services de diagnostic			X	X		X	
Mise à jour de la liste des utilisateurs				X	X		

[9] Les utilisateurs peuvent utiliser n'importe lequel de ces outils

3.1.2 Equipements ou programmes tiers

Certains équipements ou programmes tiers s'authentifient auprès de la ToE à l'aide d'un certificat électronique.

Le nom commun du certificat électronique détermine les droits d'accès sur les éléments suivants :

- Lecture / écriture des données métier
- Acquittement des alarmes
- Mise à jour de la liste des utilisateurs

Noms communs des certificats électroniques octroyant des droits d'accès :

Nom commun	**Equipement ou programme tiers**
product.*	**Un autre S4W**
scada.*	**Poste Central de Télégestion**
mngt.*	**S4-Manager**

Droits d'accès, selon le nom commun du certificat électronique de l'équipement distant :

Fonction accessible	**Nom commun**		
	product.*	scada.*	mngt.*
Lecture des données métier	X	X	
Ecriture des données métier	X	X	
Acquittement des alarmes		X	
Mise à jour de la liste des utilisateurs			X

3.2 Hypothèses sur l'environnement

Les hypothèses suivantes sont formulées sur l'environnement et les conditions d'utilisation de la ToE :

- **H.Lecture des journaux** : Il est considéré que les administrateurs consultent régulièrement les journaux locaux ou déportés générés par l'équipement.
- **H.Administrateurs :** les administrateurs de la ToE sont compétents, formés et non hostiles. Il s'agit :
  - Des personnes physiques possédant le profil utilisateur « **Administrateur** » ou « **Manager** » (Administration de la ToE au travers de de l'outil **S4W-Tools**).
  - De l'administrateur de S4-Manager.
- **H.Local ToE** : la ToE est installée soit dans une armoire électrique implantée dans un local technique sécurisé, soit dans une armoire double enveloppe sécurisée. Dans tous les cas, l'accès est restreint à des personnes autorisées et donc considérées comme non hostiles. L'attaquant n'aura pas accès aux ports physiques de la ToE.
  En revanche, des équipements identiques à la ToE étant disponibles à la vente (par notre propre réseau de distribution), l'attaquant peut acheter un tel équipement en vue d'y rechercher des vulnérabilités par tous les moyens à sa disposition pour attaquer la ToE.
- **H.Local autres S4W** : tous les S4W appartenant au réseau sont installés soit dans une armoire électrique implantée dans un local technique sécurisé, soit dans une armoire double enveloppe sécurisée.
- **H.Services non évalués désactivés par défaut** : l'ensemble des services présents dans la ToE, mais hors de la cible de sécurité, sont désactivés dans la configuration par défaut (configuration usine).
- **H.Documentation de sécurité** : la ToE est fournie avec une documentation détaillée sur l'utilisation sécurisée de l'équipement. En particulier, l'ensemble des secrets de connexion présents par défaut est listé pour permettre leur personnalisation.
  L'ensemble des préconisations issues de cette documentation seront appliquées en vue de l'évaluation.
- **H.Paramètres fixes de la ToE** : l'initialisation des paramètres de la ToE (contenus dans les composants RFID) est effectuée durant la fabrication. Cette procédure est considérée comme non compromise.
- **H.Réseau de terrain** : le réseau de terrain de la ToE, sur lequel sont présents les équipements déployés sur son propre réseau de terrain, est considéré de confiance.
- **H.VPN** : l'utilisateur installe sur le réseau de supervision un serveur VPN de confiance, compatible OpenVPN.
- **H.Managé** : la gestion des utilisateurs s'effectue exclusivement via l'outil S4-Manager.
- **H.Génération de la clé privée** : la clé privée stockée dans le composant sécurisé est générée à l'usine de fabrication du composant. Cette procédure est considérée comme fiable et non compromise.

4. DESCRIPTION DES BIENS SENSIBLES A PROTEGER

4.1 Biens sensibles de l'environnement

Les biens sensibles de l'environnement sont les suivants :

- **B.Commande du procédé industriel** : la ToE participe à la commande et au contrôle d'un processus industriel en lisant des entrées et en envoyant des ordres aux actionneurs. Ces actions doivent être protégées en disponibilité et en intégrité.
- **B.Échanges entre la ToE et le Poste Central de Télégestion** : les échanges entre le Poste Central de Télégestion et la ToE sont nécessaires au bon fonctionnement du système industriel dans son ensemble. Ceux-ci doivent-être protégés en intégrité, en confidentialité et en authenticité.
- **B.Échanges entre la ToE et les outils d'administration** : les flux entre la ToE et ces outils doivent être protégés en intégrité, en confidentialité et en authenticité.
- **B.Échanges entre la ToE et les outils d'exploitation** : les flux entre la ToE et ces outils doivent être protégés en intégrité, en confidentialité et en authenticité.
- **B.Échanges entre la ToE et un autre S4W** : pour les communications entre la ToE et un autre **S4W** doivent être protégées en intégrité, en confidentialité et en authenticité.

Les besoins de sécurité pour les biens sensibles de l'environnement sont les suivants :

Biens sensibles de l'environnement	**Disponibilité**	**Confidentialité**	**Intégrité**	**Authenticité**
B.Commande du procédé industriel	X		X	
B.Échanges entre la ToE et le Poste Central de Télégestion		X	X	X
B.Échanges entre la ToE et les outils d'administration		X	X	X
B.Échanges entre la ToE et les outils d'exploitation		X	X	X
B.Échanges entre la ToE et un autre S4W		X	X	X

4.2 Biens sensibles de la ToE

Les biens sensibles de la ToE sont les suivants :

- **B.Logiciel** : afin d'assurer correctement ses fonctions, le logiciel de la ToE est intègre et authentique.
- **B.Configuration** : la configuration de la ToE est confidentielle, intègre et authentique. L'attaquant ne peut découvrir cette configuration que par l'observation de l'activité de la ToE.

  La configuration de la ToE peut contenir un programme d'automatisme additionnel, écrit et chargé par un utilisateur.

  La configuration contient les certificats électroniques (certificat de la ToE, certificat de l'autorité de confiance, liste de révocation).
- **B.Mode de fonctionnement de la ToE** : le mode de fonctionnement de la ToE doit être protégé en intégrité.
- **B.Mécanisme d'authentification des utilisateurs** : ce mécanisme s'appuie sur une base de données locale qui est mise à jour automatiquement avec S4-Manager. La ToE doit protéger l'intégrité et l'authenticité du mécanisme.
- **B.Secrets de connexion des utilisateurs** : il s'agit de mots de passe pour les personnes physiques. Les empreintes de ces mots de passe sont contenues dans la ToE et peuvent être mises à jour par S4-Manager. La ToE garantit l'intégrité et la confidentialité de ces identifiants.
- **B.Clé privée** : clé privée associée au certificat électronique de la ToE. Cette clé doit rester confidentielle et intègre.
- **B.Politique de gestion des droits** : cette politique est fixée dans la ToE. La ToE doit garantir l'intégrité de cette politique de gestion des droits.
- **B.Fonction de journalisation locale** : la ToE dispose d'une fonction de journalisation locale qui, une fois configurée, doit rester opérationnelle. Ce journal se consulte à l'aide du logiciel S4-View, au travers du support de communication USB Device, Ethernet, ou GSM.
- **B.Fonction de journalisation distante** : la ToE dispose d'une fonction de journalisation vers un **serveur Syslog**, qui une fois configurée, doit rester opérationnelle.
- **B.Journal d'évènements local** : le journal local généré par la ToE doit être intègre, confidentiel et authentifié.
- **B.Journal d'évènements déporté** : le journal déporté émis par la ToE doit être intègre, confidentiel et authentifié. Un mécanisme doit également permettre au destinataire de détecter l'absence d'un message au sein d'une séquence de messages correctement reçus.
- **B.Paramètres fixes de la ToE :** la ToE est livrée avec des paramètres « produit », initialisés à l'usine de fabrication (N° de série, adresse MAC, code IMEI, …). Ceux-ci ne sont pas modifiables par l'utilisateur. Ces paramètres stockés dans les composants RFID doivent rester intègres.
- **B.Données métier :** variables, archives, ou alarmes contenues dans la ToE.

Les variables sont utilisées pour mémoriser les états courants des E/S locales, les données communiquées par un équipement tiers (niveau d'eau, température, pression, …), ou les résultats d'un traitement sur d'autres variables.

La ToE doit garantir l'intégrité et la confidentialité de ces données métier.

Les besoins de sécurité pour les biens sensibles de la ToE sont les suivants :

Biens sensibles de la ToE	Disponibilité	Confidentialité	Intégrité	Authenticité
B.Logiciel			X	X
B.Configuration		X	X	X
B.Mode de fonctionnement de la ToE			X	
B.Mécanisme d'authentification des utilisateurs			X	X
B.Secrets de connexion des utilisateurs		X	X	
B.Clé privée de la ToE		X	X	
B.Politique de gestion des droits			X	
B.Fonction de journalisation locale	X			
B.Fonction de journalisation distante	X			
B.Journal d'évènements local		X	X	X
B.Journal d'évènements déporté		X	X	X
B.Paramètres fixes de la ToE			X	
B.Données métier		X	X	

4.3 Description de la menace

4.3.1 Description des agents menaçants

Les agents menaçants suivants ont été retenus :

- **Attaquant sur le réseau de supervision** : l'attaquant a la maîtrise d'un équipement sur le réseau de supervision de la ToE.
- **Attaquant sur le réseau local** : l'attaquant a la maîtrise d'un équipement sur le réseau local (LAN) de la ToE.
- **Attaquant sur le réseau opérateur** : l'attaquant a la maîtrise d'un équipement sur le réseau opérateur (WAN).
- **Utilisateur malveillant** : l'attaquant a réussi à compromettre un compte sans privilèges d'administration et cherche à outrepasser les droits de son compte.

4.3.2 Menaces retenues

Les menaces suivantes ont été retenues :

- **M.Déni de service :** l'attaquant parvient à effectuer un déni de service sur la ToE en effectuant une action imprévue ou en exploitant une vulnérabilité (envoi d'une requête malformée, utilisation d'un fichier de configuration corrompu …). Ce déni de service peut concerner toute la ToE ou seulement certaines de ses fonctions.
- **M.Corruption du logiciel :** l'attaquant parvient à injecter et faire exécuter un logiciel corrompu sur la ToE. L'injection de code peut être temporaire ou permanente et ceci inclut donc toute exécution de code non prévue ou non autorisée. L'attaquant peut également réussir à substituer une mise à jour corrompue à une mise à jour légitime. Un utilisateur pourra alors tenter d'installer cette mise à jour dans la ToE par des moyens légitimes. Enfin, l'attaquant peut également tenter d'installer une version légitime du logiciel sans en avoir le droit.
- **M.Corruption du mode de fonctionnement de la ToE :** l'attaquant parvient à modifier le mode de fonctionnement de la ToE sans en avoir le droit (envoi d'une commande stop par exemple).
- **M.Corruption de la configuration :** l'attaquant parvient à modifier, de façon temporaire ou permanente, la configuration de la ToE.
- **M.Compromission de la configuration :** l'attaquant parvient à récupérer tout ou partie de la configuration de la ToE de manière illégitime.
- **M.Vol d'identifiants :** l'attaquant parvient à récupérer ou modifier les secrets de connexion d'un utilisateur.
- **M.Compromission de la clé privée de la ToE :** l'attaquant parvient à récupérer ou modifier la clé privée de la ToE.
- **M.Contournement de l'authentification :** l'attaquant parvient à s'authentifier sans avoir les secrets de connexion.
- **M.Contournement de la politique de droits :** l'attaquant parvient à obtenir des droits qui ne lui sont pas normalement dévolus.
- **M.Corruption du journal d'évènements local** : l'attaquant parvient à supprimer ou modifier une entrée dans le journal local sans y avoir été autorisé par la politique de droits de la ToE.
- **M.Compromission du journal d'évènements local** : l'attaquant parvient à récupérer tout ou partie du journal local de la ToE de manière illégitime.
- **M.Corruption du journal d'évènements déporté** : l'attaquant parvient à modifier une entrée du journal distant émise par la ToE sans que le destinataire ne puisse s'en rendre compte. L'attaquant parvient à supprimer une entrée du journal distant sans que le destinataire ne puisse s'en rendre compte.
- **M.Compromission du journal d'évènements déporté** : l'attaquant parvient à récupérer tout ou partie du journal d'évènements déporté de la ToE de manière illégitime.

- **M.Injection de commandes ou paramètres** : l'attaquant parvient à modifier des paramètres à l'intérieur de la ToE ou de lui passer des commandes sans y être autorisé.
- **M.Altération des flux :** l'attaquant parvient à modifier des échanges entre la ToE et un composant externe sans que cela ne soit détecté.
- **M.Compromission des flux :** pour les flux requérant la confidentialité, l'attaquant parvient à récupérer des informations en interceptant des échanges entre la ToE et un composant externe.
- **M.Corruption des paramètres de la ToE :** l'attaquant parvient à corrompre les paramètres fixes de la ToE (modification du N° de série …) à distance[10].
- **M.Corruption des données métier :** l'attaquant parvient à modifier, de façon temporaire ou permanente, une donnée métier contenue dans la ToE (ex : niveau d'eau).
- **M.Compromission des données métier :** l'attaquant parvient à récupérer tout ou partie des données métier contenues dans la ToE (ex : niveau d'eau).

[10] Les hypothèses « H.Local ToE » et « H.Local autres S4W » rendent impossible l'attaque via le canal radio.

4.4 Fonctions de sécurité

Les fonctions de sécurité mises en œuvre sont les suivantes :

- **F.Gestion des entrées malformées** : la ToE a été développée de manière à gérer correctement les entrées malformées, en particulier en provenance du réseau.
- **F.Stockage sécurisé des secrets** : les secrets de connexion des utilisateurs sont stockés de manière sécurisée sur la ToE et la compromission d'un fichier ne permet pas de les récupérer.
- **F.Authentification sécurisée sur les interfaces d'administration et d'exploitation** : les jetons de session sont protégés contre le vol et contre le rejeu. Les jetons de session ont une durée de vie limitée. L'identité du compte utilisé est vérifiée systématiquement avant toute action privilégiée.
- **F.Politique de droits** : la politique de gestion des droits est gérée de manière extrêmement stricte. L'implémentation de cette politique permet en particulier de garantir l'authenticité des opérations critiques, c'est-à-dire pouvant porter atteinte aux biens sensibles identifiés.
- **F.Signature du logiciel** :

  A chaque installation d'un nouveau logiciel, l'intégrité et l'authenticité de celui-ci sont vérifiées.

  A chaque démarrage de la ToE, l'intégrité du logiciel est vérifiée.

  Note : le bootloader est écrit lors de la phase de fabrication. Celui-ci n'est par la suite pas remplacé.
- **F.Intégrité et confidentialité de la configuration** : la politique de gestion des droits utilisateurs ne permet à une personne non autorisée, ni de lire, ni d'écrire tout ou partie de la configuration de la ToE.
- **F.Intégrité des commandes du mode de fonctionnement** : la ToE doit garantir que le mode de fonctionnement ne pourra être modifié que par des personnels autorisés et donc authentifiés.
- **F.Communications sécurisées** : la ToE permet l'usage de communications sécurisées, protégées en intégrité, en authenticité et en confidentialité avec des composants externes.
- **F.Intégrité du journal local** : le journal d'événements généré par la ToE est intègre et seul l'administrateur peut les modifier.
- **F.Intégrité du journal déporté** : la ToE permet de transmettre le journal déporté à un équipement tiers de manière intègre, authentifiée, et sans rejeu, avec détection des événements manquants.
- **F.Intégrité des paramètres de la ToE** : les puces RFID utilisées par la ToE sont configurées pour empêcher l'écriture, de sorte qu'il ne soit pas possible d'en modifier le contenu en dehors de l'usine de fabrication.

5. ANNEXES

5.1 Couverture des biens par les menaces

	B.Commande du procédé industriel	B.Échanges entre la ToE et le Poste Central de Télégestion	B.Échanges entre la ToE et les outils d'administration	B.Échanges entre la ToE et les outils d'exploitation	B.Échange entre la ToE et un autre S4W	B.Logiciel	B.Configuration	B.Mode de fonctionnement de la ToE	B.Mécanisme d'authentification des utilisateurs	B.Secrets de connexion des utilisateurs	B.Clé privée de la ToE	B.Politique de gestion des droits	B.Fonction de journalisation locale	B.Fonction de journalisation distante	B.Journal d'évènements local	B.Journal d'évènements déporté	B.Paramètres fixes de la ToE	B.Données métier
M.Déni de services	D												D	D				
M.Corruption du logiciel						IA												
M.Corruption du mode de fonctionnement de la ToE								I										
M.Corruption de la configuration							IA											
M.Compromission de la configuration							C											
M.Vol d'identifiants										CI								
M.Compromission de la clé privée de la ToE											CI							
M.Contournement de l'authentification									IA									
M.Contournement de la politique de droits												I						
M.Corruption du journal d'évènements local															IA			
M.Compromission du journal d'évènements local															C			
M.Corruption du journal d'évènements déporté																IA		
M.Compromission du journal d'évènements déporté																C		

	B.Commande du procédé industriel	B.Échanges entre la ToE et le Poste Central de Télégestion	B.Échanges entre la ToE et les outils d'administration	B.Échanges entre la ToE et les outils d'exploitation	B.Échange entre la ToE et un autre S4W	B.Logiciel	B.Configuration	B.Mode de fonctionnement de la ToE	B.Mécanisme d'authentification des utilisateurs	B.Secrets de connexion des utilisateurs	B.Clé privée de la ToE	B.Politique de gestion des droits	B.Fonction de journalisation locale	B.Fonction de journalisation distante	B.Journal d'évènements local	B.Journal d'évènements déporté	B.Paramètres fixes de la ToE	B.Données métier
M.Injection de commandes ou paramètres	DI	IA	IA	IA														
M.Altération des flux	DI	IA	IA	IA	IA													
M.Compromission des flux		C	C	C	C													
M.Corruption des paramètres de la ToE	D																I	
M.Corruption des données métier																		I
M.Compromission des données métier																		C

5.2 Couverture des menaces par des objectifs de sécurité

	M.Déni de services	M.Corruption du logiciel	M.Corruption du mode de fonctionnement de la ToE	M.Corruption de la configuration	M.Compromission de la configuration	M.Vol d'identifiants	M.Compromission de la clé privée de la ToE	M.Contournement de l'authentification	M.Contournement de la politique de droits	M.Corruption du journal d'évènements local	M.Compromission du journal.d'évènements local	M.Corruption du journal d'évènements déporté	M.Compromission du journal d'évènements déporté	M.Injection de commandes ou paramètres	M.Altération des flux	M.Compromission des flux	M.Corruption des paramètres de la ToE	M.Corruption des données métier	M.Compromission des données métier
F.Gestion des entrées malformées	X																		
F.Stockage sécurisé des secrets						X	X												
F.Authentification sécurisée sur les interfaces d'administration et d'exploitation						X		X	X										
F.Politique de droits				X	X					X	X							X	X
F.Signature du logiciel		X																	
F.Intégrité et confidentialité de la configuration				X	X														
F.Authenticité et intégrité des commandes du mode de fonctionnement			X																
F.Communications sécurisées						X						X	X	X	X	X		X	X
F.Intégrité du journal local										X									
F.Intégrité du journal déporté											X								
F.Intégrité des paramètres de la ToE	X																X		